ارزیابی خطر ناشی از تهدیدهای کنترل داخلی در سیستم‌های اطلاعاتی حسابداری مبتنی بر رایانه

دکترمحمد عرب‌مازاریزدی
دانشیار دانشگاه شهیدبهشتی
یاور خسروی
دانشجوی کارشناسی ارشد حسابداری

خلاصه

تحولات سال‌های اخیر در عرصه فناوری اطلاعات با آثار بسیار گسترده‌ای بر سیستم‌های اطلاعاتی حسابداری همراه بوده است. کمتر سازمان یا شرکتی را می‌توان یافت که بهره‌گیری از نظام‌های اطلاعاتی استقرار یافته بر مبنای فناوری‌های نوین را تجربه نکرده باشد. طبعاً استفاده از این سیستم‌ها با مخاطرات جدیدی نیز همراه است. مدیران باید مترصد شناسایی خطرات بالقوه ناشی از تهدیدات کنترل داخلی موجود در سیستم‌های اطلاعات حسابداری مبتنی بر رایانه باشند و با استفاده از انواع مدل‌ها، آثار این مخاطرات را ارزیابی کنند. در راستای تدوین و اجرای خط‌مشی‌ها و رویه‌های جدید سیستم کنترل‌های داخلی برای حفاظت از سیستم‌های اطلاعاتی به شیوه‌ای منسجم و مطمئن، ارزیابی چنین خطراتی ضروری به نظر می‌رسد.

مقدمه

افزایش رقابت جهانی و تغییرات مداوم در فناوری پردازش اطلاعات، برای مدیران و حسابرسان مسئول پیاده‌سازی، ایجاد و نظارت بر معیارهای کنترل داخلی در سازمان، چالش‌های جدیدی را به‌وجود می‌آورد. از طرف دیگر، بسیاری از سازمان‌ها به‌دلیل تغییرات سریع رخ داده، دریافته‌اند که تحصیل مهارت‌های تکنیکی به منظور اعمال سیاست‌ها و رویه‌های کنترلی مشکل می‌باشد. فناوری اطلاعاتی، فرصت‌های ویژه‌ای را برای حل مسائل تجاری راهبردی و فنی ارائه می‌کند. اما دروازه فناوری اطلاعات همیشه به روی تهدیدات سیستم کنترل داخلی باز است و بالطبع در معرض خطراتی قرار می‌گیرد که برای سیستم‌های اطلاعاتی حسابداری پذیرفتنی است. برای نمونه، از تهدیدات جدیدی می‌توان نام برد که به‌دلیل افزایش تعداد کاربران رایانه ایجاد می‌شود. خطر ناشی از تهدیدات بالقوه کنترل‌های داخلی موجود در سیستم اطلاعاتی حسابداری مبتنی بر رایانه باید ارزیابی شود. این ارزیابی از خطر برای تصمیم‌گیری مناسب در مورد ایجاد رویه‌ها و سیستم‌های کنترل داخلی جدیدی ضروری است که برای حفاظت یکپارچه و مطمئن از سیستم‌های اطلاعاتی، مستقر می‌شود.

ارزیابی خطرات مربوط به تهدیدات سیستم کنترل داخلی سازمان معمولاً جزیی ضروری از کار حسابرسان بوده است. به هرحال، قانون ساربینز-اکسلی(۲۰۰۲) مسئولیت پیاده سازی، نگهداری و ارزیابی سیستم کنترل‌های داخلی را به مدیریت واگذار و آنها را ملزم کرده تا ارزیابی اثربخشی کنترل‌های داخلی را در گزارش سالانه شرکت مد نظر قرار دهند. بنابراین مدیران مجبورند که

مستقیماً به مراقبت از کیفیت داده‌ها و جلوگیری از تخلفات سیستم کنترل داخلی بپردازند. کیفیت داده‌ها شامل مشخصه‌هایی مانند صحت[1]، به‌موقع بودن[2]، دقت(صراحت)[3]، قابلیت اتکا[4] و اطمینان، کامل بودن[5]، قابلیت دسترسی[6] و قابلیت تفسیر[7] در مرحله طراحی سیستم‌هایی است که از طریق مشارکت دادن کاربران در فرایند طراحی صورت می‌گیرد. بنابراین کمبودهای موجود در کیفیت داده‌ها، گرچه مستقیماً باعث بروز مشکل در سیستم کنترل داخلی نمی‌شوند اما می‌توانند در پیش‌بینی اطلاعات ضروری برای تصمیم‌گیری‌ها، ضعف و اختلال ایجاد کنند.

در محیط پردازش اطلاعات مبتنی بر رایانه، جلوگیری از نقایص سیستم کنترل‌های داخلی مستلزم توجه به موضوعات مهمی چون شناخت خطر امنیت، یکپارچگی و حساسیت داده‌ها است. از این نظر، رویه‌های حسابرسی داخلی عادی برای مواجه شدن با چنین چالش‌هایی ناکافی است. برای نمونه، رویه‌های حسابرسی اغلب ممکن است برای آشکار کردن یا کشف اعمال عمدی مانند اختلاس یا تقلب، کافی نباشد. بر همین اساس، مدیران امروزه در محیط پردازش اطلاعات رایانه‌ای مجبورند تا خطراتی شناسایی و ارزیابی کنند که کنترل داخلی را تهدید می‌کند.

هدف اصلی مدیران در ارزیابی خطرات سیستم کنترل داخلی این است که پایه‌های منطقی استقرار رویه‌های کنترل داخلی جدید را اثبات و توجیه کنند. فرایند اتخاذ تصمیم مربوط به استقرار خط مشی‌ها و رویه‌های کنترل داخلی مناسب، به‌طور قابل ملاحظه‌ای هزینه‌های مربوط به حسابرسی داخلی سازمان را کاهش می‌دهد. مشکل عمده در ارزیابی خطرات تهدیدکننده کنترل داخلی این است که نمی‌توان آن را به صورت کمی بیان کرد. بنابراین مشاوران برون‌سازمانی و مدیران برای مطالعات پرسشنامه‌ای مجبورند به پاسخ‌های شفاهی استفاده‌کنندگان سیستم اتکا کنند. این پاسخ‌های شفاهی نیز معمولاً با عدم قطعیت و ابهام همراه است.

عدم قطعیت در پاسخ‌ها، ناشی از این واقعیت است که تهدیدات سیستم کنترل داخلی، از نظر ماهیت، احتمال وقوع دارند و ممکن است احتمال وقوع آنها به طور دقیق قابل پیش‌بینی نباشد. ابهام در پاسخ سؤالات پرسیده شده را می توان به مواردی از قبیل عدم دقت در توضیحات شفاهی، مانند احتیاط و محافظه‌کاری به هنگام پاسخ‌گویی[8] یا وجود موضوعات بسیار محرمانه نسبت داد. منطق دو ارزشی رایج در قضاوت‌ها، کفایت لازم برای حذف عدم قطعیت و ابهام را ندارد. با استفاده از روش ارائه شده در تئوری فازی، پدیده‌های مبهم یا غیرقطعی را می‌توان مورد بررسی و قضاوت قرار داد.

موارد امنیتی در سیستم‌های حسابداری رایانه‌ای وماهیت تهدیدهای بالقوه

توسعه و اعتلای مهندسی سخت‌افزار و طراحی نرم‌افزار، بسیاری از موارد مربوط به سیستم کنترل‌های داخلی معمول در زمینه‌های قابلیت اتکا، به موقع بودن، دقت و صحت اطلاعات را تسهیل کرده است. رایانه‌های پیشرفته و بسته‌های نرم‌افزاری، علاوه بر کنترل‌های سخت افزاری، چندین کنترل کاربردی را در خود جای می‌دهند. در مراحل اولیه توسعه سیستم‌های ماشینی، تبدیل و پردازش اطلاعات به‌صورت رایانه‌ای، منجر به نوعی احساس کاذب امنیت در میان سازمان‌ها یعنی این احساس شده بود که رایانه‌ها مصون از تقلب و کلاهبرداری‌اند.(Allen, 1977) در نتیجه، تهدیدات موجود در سیستم‌های اطلاعاتی سازمان‌ها اغلب در نظر گرفته نمی‌شد و یا از اهمیت چندانی برخوردار نبود. به هر حال، تغییرات سریع فناوری در مراحل مختلف آن سبب شده تا نگرانی‌های فزاینده‌ای در زمینه مسائل بالقوه‌ای پدید آید که با فناوری‌های اطلاعاتی در ارتباط است.(Davis, 1997)

در یکی دو دهه گذشته، استفاده از رایانه در سازمان‌ها با سرعت بالایی افزایش یافته است. شبکه‌های داخلی و سیستم‌های متصل که به رایانه مرکزی یا سرور[9]، اطلاعات را بین تعداد زیادی از کاربران توزیع می‌کنند. شبکه‌های گسترده[10] (WAN) توانسته‌اند برای مشتریان و تامین‌کنندگان کالا و خدمات، شرایطی فراهم سازند که دسترسی به سیستم‌های دیگر و اطلاعات تسهیل گردد. سیستم‌های تبادل اطلاعات الکترونیک[11] به طرفین اجازه می‌دهد تا اسناد و مدارک را در یک لحظه رد و بدل کنند. سیستم کنترل‌های داخلی که می توانند مشمول چنین تغییراتی شوند هنوز در قلمرو سیستم‌های اطلاعاتی حسابداری به‌طور کامل شناسایی نشده‌اند. با این وجود، شناختی کلی از ماهیت مخاطرات کنترل‌های داخلی وجود دارد که مبتنی بر همین تغییرات است.

افزایش حجم تجارت الکترونیک و هم چنین ظهور پارادایم جدیدی در تسهیم اطلاعات بین خریداران، تامین‌کنندگان، نهادهای مالی، قسمت‌های پشتیبانی و سایر خدماتی که به

تازگی ظهور یافته‌اند، سبب شده تا پیگیری‌هایی مجدانه و همچنین تجدیدنظر در راهبردها، لزوم بیشتری یابد تا بدین وسیله از خطرات احتمالی حاکم بر امنیت و انسجام اطلاعات جلوگیری به عمل آید.

وانگ و استرانگ (Wang and Strong,1996) براین باورند که مدیران و متخصصان فناوری اطلاعات باید در جهت گسترش فعالیت‌های خود در زمینه صحت اطلاعات گام‌هایی جدی برداشته و بر اصول گسترده‌تری از کیفیت اطلاعات تمرکز کنند، یعنی بر اطلاعاتی متمرکز شوند که از نظر کیفیت برای استفاده‌کنندگان اطلاعات از اهمیت بیشتری برخوردار است.

در مطالعات قبلی، دیویس (Davis, 1997) نقطه نظرات ۳۵۵ نفر از حسابداران مستقل را بررسی کرده و به موارد زیر به‌عنوان مهم‌ترین تهدیداتی پی برده بود که در انواع محیط‌های رایانه‌ای وجود دارند:

- نابودی تصادفی اطلاعات به‌وسیله کارکنان
- ورود ویروس رایانه‌ای به سیستم
- کنترل ناکافی بر رسانه‌های ذخیره‌ای
- ثبت اطلاعات نادرست به‌صورت تصادفی توسط کارمندان
- سوانح سیاسی و طبیعی مانند آتش سوزی، سیل و جنگ
- سرعت پیشرفت‌های فناوری قبل از ایجاد کنترل‌های مناسب
- جداسازی اندک وظایف حسابداری از سیستم‌های اطلاعاتی
- دسترسی نداشتن به اطلاعات و سیستم‌ها

علاوه بر این، اشتباهات نرم‌افزاری و درست عمل نکردن تجهیزات، مانند کشف نکردن اشتباهات انتقال اطلاعات، خاموشی برق و نقصان سخت‌افزار برای سیستم‌های اطلاعاتی حسابداری، از تهدیدات جدی به حساب می‌آید (Romney and Steinbart, 2002). این نوع تهدیدات به این دلیل اهمیت دارند که انسجام، کیفیت، امنیت و قابلیت دسترسی اطلاعات را در معرض خطر قرار می‌دهند و هم‌چنین قابلیت سودآوری و شرایط رقابتی سازمان‌ها به‌طور قابل توجهی آسیب می‌بینند. تهدیدهای موجود در انسجام اطلاعات شامل تخریب صحت و قابلیت اتکای اطلاعات است. خطرات بالقوه برای امنیت اطلاعات شامل انتشار اطلاعات محرمانه و حساس به بخش‌هایی می‌باشد که مورد نظر نبوده است. زمانی که بر اثر عملی اشتباه و غیرقابل جبران، اطلاعات ضروری از پرونده‌ای پاک شود، در

آن‌صورت قابلیت دسترسی به اطلاعات به خطر می‌افتد.

اگر بتوان ۱) زیان‌های بالقوه مالی را افشا کرد، و ۲) خطراتی را تبیین کرد که به‌طور خاص از اهمیت ویژه‌ای برخوردارند، در آن‌صورت می‌توان از آنها برای تبیین خطرات مرتبط با کنترل‌های داخلی شرکت‌ها به شکل کمّی استفاده کرد. به عبارت دیگر، از نظر مادی می‌توان میزان خطرات را مشخص ساخت.

کنترل‌های سنتی نمی‌توانند، به طور کامل نیازهای کنترلی را در قلمرو ارزیابی، طراحی و پیاده‌سازی سیستم برآورده کند به نحوی که معیارهای موجود بتوانند تغییرات احتمالی مسائل امنیتی سازمان را به خوبی مدیریت کند. بنابراین یکی از پیش‌نیازهای ضروری برای طراحی و پیاده‌سازی رویه‌های کنترلی، شناسایی ماهیت تهدیداتی است که سیستم‌های اطلاعاتی حسابداری با آنها روبه‌رو می‌شود زیرا اتفاقات تصادفی مربوط به تهدیدات مختلف، دارای اشکال متفاوتی است و مدیران باید قبل از پیاده‌سازی ضوابط کنترل داخلی، اطلاعات قابل اتکا و موثقی را در مورد احتمال و توجیه هزینه فایده سیستم مربوطه به‌دست آورند.

برآورد هزینه پیاده‌سازی رویه‌های کنترل، امری نسبتاً آسان اما برآورد مزایای مربوط به کنترل در قالب ارقام پولی کاملاً مشکل است زیرا روش سرراست و ساده‌ای برای نتیجه گرفتن از چنین برآوردهایی وجود ندارد. بخاطر فقدان شواهد عینی از مزایای کنترل و به دلیل هزینه‌های بسیار بالای اندازه‌گیری آن، اغلب مدیران مجبورند از پیاده‌سازی معیارهای سنجش کنترل داخلی صرف نظر کنند. یکی از راه‌های ممکن برای تعیین مزایای رویه‌های کنترل داخلی، ارائه برآوردی از زیان‌هایی است که شرکت‌ها در صورت پیاده نکردن سیستم‌های کنترل داخلی متحمل می‌شوند. مهم‌ترین موضوع در این فرایند، این است که ارزیابی خطر مربوط به کنترل‌های داخلی بدون افشای زیان آن نمی‌تواند به‌طور قطعی قابل اطمینان باشد. برای انجام این کار، اغلب از مشاوران مالی برون‌سازمانی استفاده می‌شود. علاوه برگران بودن چنین فرایندی، مشکلی که در زمینه اعتماد به مشاوران بیرونی وجود دارد این است که آنها به‌ندرت، کارکنان سازمان را در بررسی‌های خود دخالت می‌دهند. کارکنان سازمان نیز به دلیل مشارکت نداشتن، اغلب متوجه اهمیت تهدیدات محتمل نیستند. بنابراین با وجود آن که معیارهای کنترل از قبل تعیین شده‌اند اما اغلب استفاده‌کنندگان نسبت به پیاده‌سازی و اجرای آنها بی‌میل هستند.

در سال‌های اخیر تعدادی از بسته‌های نرم‌افزاری موجود در بازار به حسابداران حرفه‌ای و مشتریانشان در زمینه تحلیل احتمال خطر انواع مختلف تهدیدات و ارزیابی مربوط به مزایای راه حل‌های چنین تهدیداتی، کمک می‌کنند. برای مثال **انجمن حسابداران رسمی امریکا**[12] و **انجمن حسابداران خبره کانادا**[13] خدمت تازه‌ای در مورد ارزیابی سیستم‌ها ارائه کرده‌اند که Systrust نامیده می‌شود و در مورد قابلیت اتکای سیستم اطلاعات حسابداری شرکت‌ها اطمینان می‌دهد. آنها هم چنین برنامه‌ای در ارتباط با تجارت الکترونیک بین‌المللی نیز معرفی کرده‌اند که Webtrust نامیده می‌شود و بر موارد مرتبط با سایت مشتری در زمینه محرمانه بودن، امنیت، صحت و در دسترس بودن اطلاعات مربوط به معاملات تجارت الکترونیکی، تمرکز دارد.

تولید کنندگان نرم‌افزارهای موسوم به "**سیستم پشتیبانی تصمیم‌گیری**"[14]، نوعی از بسته‌های نرم‌افزاری را به بازار عرضه کرده‌اند که سیستمی هوشمند تلقی می‌شود و عملیات تحلیلی نیز انجام می‌دهد. نرم‌افزار مزبور اطلاعاتی در مورد تهدیدات محتمل، مبتنی بر شواهد آماری، ارائه کرده و راهبردهایی جایگزین برای راه حل‌های کنترلی موجود در سیستم را همراه با بیان مزایای آن مطرح می‌کند. نرم‌افزار دیگری در قلمرو تجزیه و تحلیل خطر عملیات داخلی[15] وجود دارد که نرم‌افزاری تجاری بوده و شامل ۱۸۰ سوال مصاحبه‌ای در ارتباط با ساختار کنترل‌های داخلی است. میزان خطر در درجه‌های زیاد، متوسط یا کم، بر مبنای چگونگی پاسخ به سوالات مزبور، محاسبه و ارزیابی می‌شود. کوک و لانگلی (Kwok and Langley, 1999) مدل رایانه‌ای منابع خطر اطلاعات[16] را به منظور تسهیل مطالعات تجزیه وتحلیل خطر، پدید آورده‌اند.

بسته‌های نرم‌افزاری تولید شده که به منظور کاهش هزینه‌های مرتبط با عملکرد تحلیل خطر، از توانایی بسیار بالایی برخوردار هستند. با این وجود این ابزار تحلیل خطر بر این فرض استوار است که خطر را به صورت اتفاقی می‌توان اندازه‌گیری کرد. اغلب استفاده‌کنندگان نسبت به پیاده‌سازی و ارائه آنها بی‌میل هستند. اخیراً چند مورد بسته نرم‌افزاری به بازار عرضه شده که به حسابداران حرفه‌ای و مشتریانشان در تحلیل احتمال خطر انواع مختلف تهدیدات و ارزیابی مربوط به مزایای راه حل‌های جایگزین، کمک می‌کنند. همچنان که قبلاً ذکر شد کارکنان معمولاً رغبتی به استفاده از معیارهای کنترلی توصیه شده از طرف‌های خارجی، نشان

نمی‌دهند. ایشان گاه اصولاً در تجزیه و تحلیل‌های بیرونی مشارکت و دخالتی هم ندارند. سال‌ها پیش از این، شرکت تولیدات شیمیایی داوکمیکال (DowChemical) در تلاش برای تغییر نگرش کاربران به سمت ارزیابی خطر، ماتریس زیر را برای کمک به درک کارکنان و ارزیابی سیستم کنترل‌های داخلی مورد استفاده قرار داده است. (Daly, 1993)

سه ستون موجود در این ماتریس، بیانگر اهداف یا صفات سه‌گانه امنیتی، یعنی یکپارچگی داده‌ها، حساسیت داده‌ها و در دسترس بودن داده‌ها می‌باشد. همراه با موارد مربوط به اهداف امنیتی، موضوعات مرتبط با کنترل‌های داخلی یعنی مواردی همچون تغییر یا تخریب داده‌های نامعتبر، افشای داده‌های نامعتبر و اطلاعات غیرقابل دسترس نیز در ماتریس داوکمیکال گنجانده شده است. ردیف‌ها در ماتریس بیانگر تهدیدات بالقوه نسبت به امنیت اطلاعات به خاطر اشتباهات تصادفی و اعمال عمدی تقلب آمیز یا سوءاستفاده‌های عمدی است.

از کارکنان مرتبط با سیستم اطلاعاتی شرکت، بازخور مرتبط با هریک از خانه‌های ماتریس اخذ می‌شود. براساس پاسخ شفاهی کارمندان به هرکدام از بخش‌های ماتریس، میزان کنترل‌هایی تعیین شدند که باید در ارتباط با مسائل امنیتی اعمال شود. یکی از مشکلات این رویکرد اعتماد کردن به پاسخ‌های شفاهی کارمندان است. پاسخ‌های شفاهی بیان‌کننده تهدیدات موجود در سیستم اطلاعاتی، معمولاً نامشخص و مبهم بوده و تفسیرهای مختلفی از آنها برداشت می‌شود. تبدیل این از پاسخ‌های نامشخص به مبالغ مشخص، بیانگر این مطلب است که با پیاده‌سازی و اجرای رویه‌های کنترل داخلی می‌توان از زیان‌های بالقوه جلوگیری به عمل آورد اما چنین عملی، کار چندان ساده‌ای نخواهد بود. بنابراین پاسخ‌های کارمندان برای هر بخش در ماتریس ممکن است یکنواخت نباشد. هر یک از کارمندان در وضعیت‌های معین تهدیداتی را در زمینه تجارب خود مشاهده می‌کنند. مجموعه‌ای از این پاسخ‌های شفاهی متفاوت، مشکلات دیگری را بیان می‌کنند. اگر بتوان چارچوبی برای پردازش اطلاعات مبهم و نامشخص ارائه داد در آن صورت مطلوبیت ماتریس تحلیل خطر به‌طور قابل ملاحظه‌ای افزایش خواهد یافت.

ضرورت استفاده از مدل‌های مبتنی بر نظریه فازی

کوروین و همکاران (Korvin et. al., 2004) در تحقیق خود، مدلی را برای ارزیابی خطر سیستم کنترل داخلی ایجاد

کردند که به مدیران در تصمیم‌گیری فعال در مورد ارائه معیارهای کنترل داخلی در سیستم‌های حسابداری رایانه‌ای کمک خواهد کرد. ارزیابی خطر کنترل داخلی به‌طور سنتی توسط حسابرسان مستقل بررسی شده است. آنها باید خطر را برای تعیین ماهیت و دامنه آزمون‌های حسابرسی ارزیابی کنند. مدل ساخته شده بر روی ماتریس تحلیل خطر پدید آمد که توسط شرکت داوکمیکال ابداع شده بود. در مدل شرکت داوکمیکال، این طور فرض شده که ارزیابی خطر انتشار تا آن درجه ارزیابی می‌شود که بر اشتباهات تصادفی یا قصور و تقلب عمدی و سواستفاده بر انسجام اطلاعات، حساسیت داده‌ها و در دسترس بودن داده‌ها تاثیر می‌گذارد. اشکال ماتریس تحلیل خطر داوکمیکال این است که هیچ شیوه‌ای را برای برخورد با ابهام ارائه نمی‌کند که ویژگی پاسخ‌های شفاهی است. آینهورن و هوگارت (Einhorn and Hogarth, 1985) این نکته را مطرح کرده‌اند که احتمالات مبهم شامل تعدادی از احتمالات است که نمی‌توان برای آنها توزیع احتمال تعریف کرد اما احتمالات معلوم آنهایی هستند که حداقل می‌توان برای آنها توزیع احتمال تعریف کرد.

روش‌شناسی منطق فازی، امکان تدوین مدلی را فراهم کرد که احتمالات مبهم با استفاده از یک دامنه موزون با قابلیت اتکای بالا نمایش داده شود. مزیت در نظر گرفتن مجموعه‌ای از مقادیر احتمالی بر مبنای یافته‌های افراد از مشاهدات تجربی، به‌جای آنکه مقادیر معینی برای هر کدام از موارد خطر، این است که یکی از مجموعه‌های مذکور می‌تواند ابهام را درفرایند ارزیابی خطر دخالت دهد.

مدل کوروین و همکاران اگر چه تنها بر افشای اطلاعات تاکید دارد اما برای هر مطالعه دیگری کاربرد دارد که در ارتباط با خطر کنترل‌های داخلی بخواهد انجام شود. این مدل را می‌توان در قلمرو موضوعات مختلف مرتبط با سنجش خطر، تحلیل نظرات کارکنان و کارشناسان سطوح مختلف شرکت، تحلیل وضعیت خطر هر نوع شرکت با هر اندازه و هر نوع سیستم اطلاعاتی به کار برد. تصمیم‌گیری در مورد پیاده‌سازی معیارهای کنترل داخلی براساس ارزیابی منطقی خطر توسط کارکنان، مدیر را در شناسایی معیار کنترل مقرون به صرفه و در نتیجه، اطمینان از انسجام و امنیت سیستم اطلاعاتی حسابداری کمک خواهد کرد.

پی‌نوشت‌ها

1- Accuracy
2- Timeliness
3- Precision
4- Reliability
5- Completeness
6- Accessibility
7- Interpretability
8- Major Concern
9- Server
10- Wide Area Network
11- Electronic Data Interchange (EDI)
12- American Institute of Certified Public Accountants (AICPA)
13- Canadian Institute of Chartered Accountants
14- Decision Support Systems
15- Internal Operations Risk Analysis
16- Risk Data Repository (RDR)

منابع و مآخذ:

1- Allen B. 1977. The biggest computer frauds: lessons for CPAs. The Journal of Accountancy (May): 52-62.

2- Daly J. 1993. The 30-minute risk analysis. Computerworld (November 29): 68.

3- Davis C. 1997. An Assessment of accounting information security. CPA Journal (March): 28-34.

4- Einhorn H, Hogarth R. 1985. Ambiguity and uncertainty in probabilistic inference. Psychological Review 92: 433-461.

5- Kwok L, Langley D. 1999. Information security management and modeling. Information Management and Computer Security 7(1): 30-40.

6- Romney M, Steinbart P. 2002. Accounting Information System, 9th edn. Prentice-Hall: Upper Saddle River, NJ.

7- Wang RY, Strong D. 1996. Beyond accuracy: what data quality means to data customers. Journal of Management Information Systems 12(4): 5-34.

8- Korvin A, Shipley m, Omer K. 2004. Assesing Risks Due To Threats to Internal Control In A Computer-Based Accounting Information Systems: A Pragmatic Approach Based On Fuzzy Set Theory, Intelligent. Systems in Accounting Finance and Management, 12,39-152.